IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

G.T., by and through next friend Liliana T. Hanlon, individually, and on behalf of all others similarly situated, Plaintiffs, v. SAMSUNG ELECTRONICS AMERICA, INC., Defendant.	Civil Action No: 1:21-cv-04976 Hon. Nancy L. Maldonado

DEFENDANT SAMSUNG ELECTRONICS AMERICA, INC.'S MOTION AND MEMORANDUM IN SUPPORT OF MOTION TO DISMISS THE AMENDED CLASS ACTION COMPLAINT

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Cases

Statutes

Rules

Defendant Samsung Electronics America, Inc. ("Samsung") moves this Court pursuant to Federal Rule of Civil Procedure 12(b)(6) to dismiss Plaintiff's Amended Class Action Complaint ("FAC") for the reasons stated in the following Memorandum of Law.

I. INTRODUCTION

Plaintiff's claims should be dismissed because her factual allegations about the operation of Samsung's photo-viewing Gallery App demonstrate that the statute upon which her claims are based—the Illinois Biometric Privacy Act, 740 ILCS 14/1 *et seq.* ("BIPA")—plainly does not apply to Samsung's technology.

BIPA is a privacy statute that was intended to address concerns with how "biometrics" were used in streamlined financial transactions and security settings and, more specifically, with the risk of identity theft that may occur when biometrics are compromised. 740 ILCS 14/5(c). As recognized in the FAC, biometrics are "permanent, biologically-unique identifier[s] associated with the individual." FAC ¶ 13; *see also* 740 ILCS 14/5(c) (describing biometrics as identifiers biologically unique to a specific individual). Biometric identifiers do not include information such as photographs or physical descriptions, and biometric information "does not include information derived from items or procedures excluded under the definition of biometric identifiers." *See* 740 ILCS 14/10. An entity that "collect[s]" or "otherwise obtain[s]" biometric identifiers or biometric information must provide written notice and obtain prior authorization. 740 ILCS 14/15(b). Once "in possession of" biometric identifiers or information, private entities must develop and publish data retention and destruction policies. 740 ILCS 14/15(a).

Plaintiff contends that Samsung violated BIPA through a function of the Samsung Gallery App, which comes pre-installed on certain Samsung mobile devices. FAC ¶¶ 5, 23. Specifically, Plaintiff alleges that the Gallery App "organizes and sorts photos based on the particular individuals who appear in those photos." *Id.* ¶ 26. Plaintiff further alleges that to accomplish this

sorting, the Gallery App uses an algorithm that scans a user's photographs for faces and "calculates a unique digital representation of each face." *Id.* ¶ 24. In this motion, Samsung refers to the data Samsung mobile devices use to group photos within the Gallery App as "Face Clustering Data." Plaintiff alleges that the Face Clustering Data is stored in a database "in the solid state memory on the user's Samsung Devices," and further speculates that the Gallery App uses that Face Clustering Data to sort and organize photos based upon the individuals who appear in them. *Id.* ¶¶ 25-26. Even accepting Plaintiff's factual allegations about the way Gallery App operates as true for purposes of this motion, both of her counts must be dismissed.

First, Plaintiff's BIPA claims fail because she has not made—and cannot make—the requisite factual allegation to show that Samsung is "in possession of," "collect[s]," "capture[s]," or "otherwise obtain[s]" the Face Clustering Data. 740 ILCS 14/15(a), (b). Plaintiff correctly asserts that the Face Clustering Data is stored only locally in the solid state memory on Plaintiff's smartphone. *See, e.g.,* FAC ¶¶ 25, 27. And that is where her well-pleaded factual allegations end. Plaintiff does not allege any facts, based on information and belief or otherwise, to establish that any mechanism exists that allows Samsung to obtain or access that locally saved data, let alone that Samsung actually retrieved or accessed the data from her device. These deficiencies are fatal to her claims. Nor can Plaintiff remedy this deficiency through amendment, as Samsung does not collect, capture or obtain this Face Clustering Data, which as Plaintiff alleges, is stored only locally on the user's device. *Id*. The Court should reject Plaintiff's effort to transform factual allegations of Samsung's control over the design of the software app into a claim that Samsung therefore controls the Face Clustering Data that is generated by and stored locally on each user's device. *See id.* ¶¶ 34-38, 53. As courts have repeatedly recognized in a variety of contexts, simply selling a device does not give the device manufacturer "possession" or "control" over what the user does

with that device. Were it otherwise, Microsoft would have possession of and control over this motion by virtue of counsel using Microsoft Word to draft it. As detailed *infra* in Section III(A), multiple courts have rejected liability of a product manufacturer and seller where the manufacturer and seller does not collect or otherwise obtain the data that is alleged to be a biometric identifier or biometric information. The same result should apply here: Plaintiff's failure to allege any facts that plausibly show Samsung obtains or even has access to any Face Clustering Data is dispositive and requires dismissal of all of her BIPA claims.

Second, Plaintiff cannot state a BIPA claim because the Face Clustering Data is not a "biometric identifier" or "biometric information" regulated under BIPA. The text and legislative history of BIPA make clear that it is intended to cover "biometrics," which are unlike "other unique identifiers" because they are "biologically ***unique to [an] individual***." 740 ILCS 14/5(c) (emphasis added). This language focusing on the nature of biometrics as a unique identifier shows that the statute applies to data that can be used to ***identify*** an individual. Although she alleges the Gallery App can sort photos based on grouping photos of the same face, FAC ¶ 26, Plaintiff does not allege that the Face Clustering Data itself identifies who the individuals are. The reason is simple: the Face Clustering Data groups similar faces; it does not and cannot identify to whom the faces belong. As Plaintiff herself alleges, while the Gallery App uses the Face Clustering Data to group photos, Plaintiff—***not*** Samsung—identified the individuals in her photos when she "tagged" them. *Id.* ¶ 64. She does not allege that she needed the Face Clustering Data to identify the people in those photos or that she used the data to do so. *See infra* Section III(B).

In sum, Plaintiff's BIPA claims fail as a matter of law. Samsung is not required to obtain consent under BIPA Section 15(b) where the complaint's factual allegations do not plausibly establish that Samsung collects or possesses BIPA-regulated data in the first place. Likewise,

Samsung is not required to publish a retention schedule under Section 15(a) where the complaint's factual allegations do not plausibly establish that Samsung possesses or retains BIPA-regulated data. And even assuming for the sake of argument that Samsung did collect, possess or retain the Face Clustering Data (it does not), Plaintiff's claims would still fail because the Face Clustering Data is not a "biometric identifier" or "biometric information" regulated under BIPA. Plaintiff's FAC should thus be dismissed in its entirety and with prejudice.

II. LEGAL STANDARD

Dismissal is warranted when a complaint fails to allege "enough facts to state a claim to relief that is plausible on its face." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007); Fed. R. Civ. P. 12(b)(6). Claims are facially plausible only "when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the Defendant is liable for the misconduct alleged." *Garrard v. Rust-Oleum Corp.*, 575 F. Supp. 3d 995, 999 (N.D. Ill. 2021) (quoting *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (internal citations omitted)). Under the *Twombly/Iqbal* standard, the Court "need not accept as true statements of law or unsupported conclusory factual allegations." *Yeftich v. Navistar*, 722 F.3d 911, 915 (7th Cir. 2013). Instead, the Court may "draw on its judicial experience and common sense" to determine "whether a complaint states a plausible claim for relief." *Iqbal*, 556 U.S. at 679.

III. ARGUMENT

Plaintiff's claims fail for two principal reasons evident from the factual allegations once stripped of their conclusory legal language. ***First***, Samsung does not collect, otherwise obtain, or have access to the Face Clustering Data—and Plaintiff does not allege facts to the contrary. Thus, BIPA's obligations regarding written consent and publication of a retention schedule do not, and logically cannot, apply. ***Second***, the Face Clustering Data (which is stored only locally on a user's

device) is not a "biometric identifier" or "biometric information" because it does not identify particular individuals.

A. Plaintiff's BIPA Claims Fail Because Samsung Does Not "Possess" or "Collect" The Face Clustering Data at Issue.

Most fundamentally, Plaintiff does not and cannot state a claim that Samsung violated either Section 15(a) or Section 15(b) of BIPA because she does not plausibly allege that Samsung collected or is in possession of the Face Clustering Data that is the subject of her claims. To state a claim under BIPA Section 15(a), Plaintiff must allege facts showing that Samsung was "in possession" of biometric data. 740 ILCS 14/15(a). BIPA does not expressly define "possession," but courts in this District have applied the term's "popularly understood meaning" as its "settled legal meaning"—that is, "possession" occurs when the defendant held the data at its disposal or exercised dominion or control over the data, which in turn depends on whether the defendant "could freely access the data" and "how [the defendant] allegedly received it." *Heard v. Becton, Dickinson & Co*., 440 F. Supp. 3d 960, 968 (N.D. Ill. Feb. 24, 2020); *see also Jacobs v. Hanwha Techwin Am., Inc.,* 2021 WL 3172967, at *3 (N.D. Ill. Jul. 27, 2021) (using the same language and citing *Namuwonge v. Kronos, Inc.*, 418 F.Supp.3d 279, 284 (N.D. Ill. 2019)). Similarly, to state a claim under Section 15(b), Plaintiff must allege facts showing that Samsung collected, captured, or otherwise obtained biometric data. 740 ILCS 14/15(b). Courts have further held that the acquisition must involve "an active step" to acquire the data. *Heard*, 440 F. Supp. 3d at 966; *Jacobs,* 2021 WL 3172967, at *2-3.

Plaintiff's own allegations show that she cannot satisfy the required elements of her BIPA claims. While Plaintiff conclusorily alleges that Samsung "indiscriminately collects Biometrics" from photographs, FAC ¶ 32, she has not alleged any *facts* to make those allegations plausible. Rather, the facts that she does plead concede that Samsung does not collect Face Clustering Data.

Plaintiff admits that Samsung "does not store or transfer" Face Clustering Data on or by means of its servers. FAC ¶ 34. Plaintiff alleges merely that the Gallery App was pre-installed on her phone, *id.* ¶ 23; that the Gallery App runs on her device and generates Face Clustering Data, *id.* ¶¶ 23, 24; and that the Face Clustering Data is stored locally on the phone's solid state memory, *id.* ¶¶ 25, 27, 34. Critically, she does ***not*** allege that Samsung itself obtained any of the Face Clustering Data, that Samsung ever accessed that data stored locally on her phone, or that Samsung even has the ability to access that data stored locally on her phone. Those gaping holes are fatal to her BIPA claims.

In the FAC, Plaintiff appears to contend that Samsung has control over, and therefore is in "possession" of, the Face Clustering Data simply because Samsung designed the Gallery App and pre-installed it on her phone, licensed the software to her to use, and does not allow her to modify the software. *See* FAC ¶¶ 23-24, 29, 31, 34-38, 53. That strained construction of the word "possession" is flatly inconsistent with the text of the statute and the precedent interpreting it. *See Heard*, 440 F. Supp. 3d at 968; *Jacobs*, 2021 WL 3172967, *3 (holding that in the BIPA context "possession occurs when someone exercises any form of control over the data or held the data at his disposal") (internal marks omitted). Conclusory allegations of Samsung's control over design decisions about pre-installed software on Plaintiff's phone do not mean that Samsung "possessed," or even could possess, data that is later generated and stored locally on Plaintiff's device while the phone is in Plaintiff's possession. *Contra* FAC ¶ 53 (confusing control over software design with control over data on individual phone). Put simply, Plaintiff has pled no factual allegations to support the contention that Samsung "possessed" the Face Clustering Data either by holding the data at its disposal or by exercising dominion or control over it. *E.g.*, *Heard*, 440 F. Supp. 3d at 968.

In *Heard*, for example, the court rejected a claim by a hospital employee that a fingerprint scanner manufacturer "possess[ed] and actively "collect[ed]" fingerprint scanning data where the employer hospital that purchased and used the scanner—***not*** the manufacturer—owned, operated, and had access to the data allegedly obtained through the scanners. *Heard*, 440 F.Supp.3d at 964, 968-969. Similarly, in *Jacobs*, the court dismissed claims that a camera manufacturer "possessed" or "controlled" data from its cameras where a department store that purchased and had the cameras installed—***not*** the manufacturer—owned, operated, and had access to the data allegedly obtained through the cameras. *Jacobs,* 2021 WL 3172967, at *3-4. Indeed, the *Jacobs* court specifically rejected the contention that the manufacturer "possess[ed]" and actively "collect[ed]" biometric data merely by virtue of designing, selling, or providing the technology alleged to have captured it. *Id.*; *see also Stauffer v. Innovative Heights Fairview Heights LLC*, 2022 WL 3139507, at *4 (S.D. Ill. Aug 5, 2022) (dismissing Section 15(b) claim where plaintiff did not "allege that [defendant franchisor] itself stored biometric information on its own computers or servers, or that [defendant] used the biometric information for its own purposes. In fact, Plaintiff does not allege that [defendant] actually accessed this information."). Here, Plaintiff's own factual allegations show that Samsung is in the same position as the defendants in *Heard*, *Jacobs*, and *Stauffer*: while Samsung may have supplied the functionality that was used by the end user, it does not receive or have the ability to access the data that the user generates. *See* FAC ¶¶ 25, 34.

Plaintiff may point the Court to certain cases where BIPA claims have survived motions to dismiss. The allegations and reasoning in those cases actually confirm why Plaintiff's allegations are fatally deficient. In *Hazlitt v. Apple*, for example, the court allowed BIPA claims to survive a motion to dismiss based on the court's understanding that plaintiff had alleged that Apple could access the data at issue. *See* 500 F. Supp. 3d 738, 751-52 (S.D. Ill. 2020) (*"Hazlitt I*") ("[I]f what

Plaintiffs allege is true, [Apple] collects the biometric data into a facial recognition database on the device that ***Apple alone can access.***") (emphasis added) (distinguishing *Heard* and other cases); *Hazlitt v. Apple, Inc.*, 543 F. Supp. 3d 643, 653 (S.D. Ill. 2021) ("*Hazlitt II*") ("Plaintiffs also claim . . . that Apple alone could access the biometric data or disable its collection"). But despite its view of the plaintiff's claims at issue against Apple there, in *Hazlitt I*, the court confirmed access was a key issue for maintaining a BIPA claim, noting that "[a]s the facts develop, it may be that Apple cannot access any data stored on the device via its software or otherwise." *Hazlitt I*, 500 F. Supp. 3d at 751. This key premise is further underscored in later proceedings in *Hazlitt*, where an amended complaint alleged expressly that "Apple automatically transfers [the] Sync Data . . . [at issue] to Apple's servers via the cloud" and that "Apple maintains and stores encryption keys that enable it to access the Sync Data." *Hazlitt v. Apple*, No. 3:20-CV-421-NJR, Dkt. 135 at 11 (S.D. Ill. Aug. 1, 2022) Dkt. 135 at 11 (ruling on subsequent motion to dismiss) ("*Hazlitt III*"). Plaintiff here alleges the exact opposite—*i.e.,* that "Samsung does not store or transfer all user Biometrics on or by means of its servers," FAC, ¶ 34—and her inability to make a similar allegation in good faith dooms her BIPA claims. In contrast, Plaintiff here not only alleges that the Face Clustering Data remains on her phone and is not transmitted to Samsung, FAC ¶¶ 24-25 & 34, but she also makes no factual allegation that Samsung has any encryption keys or ability to access that data that resides on her phone.

Similarly, in *Namuwonge*, an employee alleged that a workforce timekeeping device manufacturer was liable under BIPA, even though his employer owned and operated the devices. *Namuwonge*, 418 F. Supp. 3d at 283, 285. The court dismissed the Section 15(b) claim because the plaintiff had failed to allege facts showing that the manufacturer actively collected biometric data. *Id.* at 286. And while the court allowed the Section 15(a) claim to survive, it did so because

the plaintiff alleged that the employer "disclosed . . . employees' fingerprint data to [the manufacturer]," which the court reasoned sufficient to establish "possession" under BIPA. *Id.* at 284. The reasoning of *Namuwonge* and *Hazlitt* thus provides additional support for the dismissal of the complaint here. Moreover, adopting Plaintiff's view that Samsung possessed information it never received and could not even access is illogical under Section 15(a). Section 15(a) requires a private entity "in possession of biometric identifiers or biometric information" to permanently destroy such information within no more than three years of the individual's last interaction with the entity. 740 ILCS 14/15(a). If creating an app that processes Face Clustering Data locally on devices were deemed to be the same as having "possession" of the data that remains solely within that individual device, Samsung would have to build capabilities (a) to continually monitor its customers' use of its devices to determine the last date of use of the Gallery App, and then for a further three years, and (b) to then access the device and permanently destroy the data stored in it by the user. This is clearly not what BIPA requires or was intended to address.

Against this backdrop, it is no wonder that multiple courts have rejected the suggestion that a technology manufacturer is *per se* in possession of user-generated biometric data by virtue of having developed the relevant tool. *E.g.*, *Heard*, 440 F. Supp. 3d at 966 (dismissing BIPA claim); *Jacobs*, 2021 WL 3172967, at *3 (same). In addition, several more cases decided since *Hazlitt I* and *II* confirm that the inquiry under Sections 15(a) and (b) turns on whether the plaintiff adequately alleged that the defendant ***itself*** accessed, collected, or possessed the alleged biometrics. *Compare Stauffer*, 2022 WL 3139507, at *4 (dismissing Section 15(b) claim where plaintiff did not allege that defendant stored, used, or accessed biometric information); *with Karling v. Samsara Inc.*, 2022 WL 2663513, at *6 (N.D. Ill. July 11, 2022) (finding plaintiff adequately stated Section 15(b) claim where it alleged that defendant "stored [plaintiff's] biometric

information in its cloud-based dashboard, and then provided access to that dashboard and services based on that data to his employer"). No factual development is needed because the factual allegations in the complaint here suffice to establish the deficiency of the claim.

Nor can Plaintiff remedy this deficiency with her conclusory contention that Samsung is vicariously liable for BIPA violations on the theory that Samsung's software and devices function as a "software agent." FAC ¶¶ 54-56. Plaintiff's theory of vicarious liability has no basis in fact or law. As an initial matter, Plaintiff has not plausibly alleged facts that the Gallery App is an agent working on behalf of Samsung as a principal to collect or possess data, where Samsung does not receive or have access to the Face Clustering Data from the device. Nor does vicarious liability law support finding that software is an "agent" of the software designer. Indeed, the Restatement on Agency upon which the complaint relies, *id.* ¶ 55, expressly states that "a computer program is not capable of acting as a principal or agent" because "computer programs are instrumentalities of the persons who use them." Restatement (Third) Of Agency § 1.04, Cmt. E (2006). Similarly, the complaint relies on *NetFuel, Inc. v. F5 Networks, Inc.*, 2017 WL 2834538, at *1 (N.D. Ill. June 29, 2017) to assert this "software agent" theory. But *NetFuel* is a patent claim construction decision that construes the technical term "software agent" as used in a particular patent; the decision did not address vicarious or agency liability at all. Plaintiff's vicarious liability theory would mean that the designer of a technology would be liable for any BIPA violations alleged to arise from the devices they designed and sold. Multiple courts have rejected similar allegations, as discussed above.

B. The Face Clustering Data at Issue Is Neither a "Biometric Identifier" Nor "Biometric Information" Because it Does Not Identify Particular Individuals.

Plaintiff's BIPA claims also fail for the independent reason that BIPA does not regulate the Face Clustering Data. BIPA regulates "biometric identifiers" and "biometric information," the

"biologically unique" data identifying specific individuals that is the focus of the statute. 740 ILCS 14/5 (discussing legislative findings and intent of BIPA). Plaintiff does ***not*** allege, nor could she, that the Face Clustering Data identifies particular individuals.

BIPA's language repeatedly reinforces that the Illinois legislature intended BIPA to protect data linked to specific individuals. The statute's section stating the "legislative findings and intent" explains: "Biometrics are unlike other unique identifiers" and they "are biologically unique to the individual." 740 ILCS 14/5(c). The use of these terms in the section about the legislative intent makes clear that the focus is on data that uniquely identifies an individual. BIPA's remaining statutory language must be interpreted accordingly. *Cf. generally Lacey v. Vill. Of Palatine*, 904 N.E.2d 18, 25 (Ill. 2009) (holding that a court must give effect to the legislature's intent as evidenced by the plain language of a statute). This intent is reinforced in the remainder of the statute. It imposes obligations with respect to "biometric ***identifiers***," a phrase that inherently by its name involves identification of an individual, and "biometric information," which is defined as "information based on an individual's biometric identifier ***used to identify an individual.***" 740 ILCS 14/10 (emphasis added). Section 15(a) requires private entities in possession of biometric data to destroy that data "when the initial purpose for collecting [it] . . . has been satisfied or within 3 years of ***the individual's*** last interaction with the private entity." 740 ILCS 14/15(a) (emphasis added). And Section 15(b) prohibits collecting, capturing, purchasing, receiving through trade, or otherwise obtaining "***a person's*** or ***a customer's*** biometric identifier or biometric information." 740 ILCS 14/15(b) (emphasis added). Accordingly, if the data cannot be used to identify a specific individual, it does not qualify as a "biometric identifier" or "biometric data."

Plaintiff failed to allege facts that the Face Clustering Data itself either identifies or can be used to identify particular individuals. Rather, she alleges that the Gallery App uses Face

Clustering Data to organize and sort photographs. FAC ¶ 26. In its discussion of the historical background of BIPA, the FAC does allege that one ***potential*** use of facial recognition technology is to match a "facial template" to an identified individual. *Id*. ¶ 20. But she makes no such allegations about the Gallery App; rather, Plaintiff alleges that the scanning feature of the Gallery App organizes or sorts the photos based on similar features, grouping together photos of the same individual, ***not*** that the Gallery App (or Samsung) identifies those photos as being of any specific, named individual. *Id.* ¶ 26. The identification of an individual takes place separately by the user of the device—specifically, Plaintiff admits in her complaint that ***she*** is the one who associated groups of photos with particular individuals by tagging photos on her device. *Id.* ¶ 64 ("[Plaintiff] has 'tagged' individuals in photographs that Samsung has organized by facial geometry"). She certainly does not allege the Face Clustering Data can identify who the individuals in the photos are; her own knowledge, not the technology, is what identifies people in her photographs. She does not (and cannot) claim that the Gallery App itself identifies the particular individuals in groups of photographs. Thus, Plaintiff has not adequately alleged that the Face Clustering Data is covered by BIPA.

Courts that have refused to dismiss BIPA claims have done so where plaintiffs alleged that the technology at issue could be, and was in fact, used to identify specific individuals, far from the allegations in the FAC. *See, e.g.*, *In re Facebook Biometric Privacy Litig.*, 185 F. Supp. 3d 1155 (N.D. Cal. 2016); *Norberg v. Shutterfly, Inc.*, 152 F. Supp. 3d 1103 (N.D. Ill. 2015); *Monroy v. Shutterfly, Inc.*, 2017 WL 4099846 (N.D. Ill. Sept. 15, 2017); *Hazlitt I*, 500 F. Supp. 3d 738; *Rivera v. Google, Inc.*, 238 F.Supp.3d 1088 (N.D. Ill. 2017). For instance, the complaints against Facebook, Shutterfly, and Google alleged that those defendants leveraged databases of face templates the defendants maintained so that defendants could actually suggest to users the identity

of the *specific* individuals appearing in their users' photographs. The *Facebook* complaint alleged that Facebook stored users' faceprints in its own database and used that data to "suggest [an] individual's name or automatically tag them" when Facebook's software recognized the face of a new photo posted to the site. *See In re Facebook*, No. 3:15-cv-03747-JD, Dkt. 40 ¶¶ 3, 43, 50 (N.D. Cal. Aug. 28, 2015). Similarly, the *Norberg* and *Monroy* complaints against Shutterfly alleged that Shutterfly's "tag suggestion" feature "works by comparing the face templates of individuals who appear in newly-uploaded photos with the facial templates already saved in Defendants' face database" and if there is a match, the software "suggests that the user 'tag' to that face the name already associated with that face." *Norberg v. Shutterfly*, No. 1:15-cv-05351, Dkt. 6 ¶ 22 (N.D. Ill. Jun. 23, 2015)); *Monroy v. Shutterfly, Inc*, No. 16-cv-10984, Dkt. 1 ¶ 23 (N.D. Ill. Nov. 30, 2016)) (substantially identical allegation). Further, the *Rivera* complaint alleged that the facial recognition technology for the cloud-based Google Photos "works by comparing the face templates of individuals who appear in newly-uploaded photos with the facial templates already saved in Google's face database" and that Google collected and used these face templates not only "to identify individuals by name, but also to recognize their gender, age, and location." *Rivera v. Google, Inc.*, No. 1:16-cv-02714, Dkt. 40 ¶¶ 22-23 (N.D. Ill. May 27, 2016)). Similarly, notwithstanding that in *Hazlitt I*, the court disagreed with the argument that the term "biometric identifier" excludes data that is not used to identify a specific person, there too the plaintiff had alleged that Apple's photos app "applies an algorithm to identify the device user." *Hazlitt I*, 500 F. Supp. 3d at 749.

But here, in contrast, Plaintiff did ***not*** allege that Samsung can or does use Face Clustering Data to identify particular individuals. It is ***the user*** who identifies who is in the clustered photos, by applying the "tag" of her choice. Not only is Plaintiff, not Samsung, identifying the individuals

in her photographs, her tag may or may not be an actual name or other identifying information. In sum, because Samsung cannot identify particular individuals using the Face Clustering Data, it is not "biometric information" or a "biometric identifier" regulated under BIPA.

IV. CONCLUSION

No factual allegations establish that Samsung engaged in any conduct prohibited under BIPA, and the Court should, therefore, dismiss Plaintiff's Amended Class Action Complaint with prejudice.

Dated: October 21, 2022

By: /s/ Randall W. Edwards
Randall W. Edwards

ATTORNEY FOR DEFENDANT
SAMSUNG ELECTRONICS AMERICA, INC.

DONOHUE BROWN MATHEWSON & SMYTH LLC
Mark H. Boyle
140 South Dearborn Street, Suite 800
Chicago, IL 60603
(312) 422-0900

O'MELVENY & MYERS LLP
Randall W. Edwards
Matthew D. Powers (*pro hac vice*)
Two Embarcadero Center, 28th Floor
San Francisco, CA 94111-3823
(415) 984-8700

O'MELVENY & MYERS LLP
Ashley M. Pavel
610 Newport Center Dr., 17th Floor
Newport Beach, CA 92660
(949) 823-6900

Attorneys for Samsung Electronics America, Inc.

CERTIFICATE OF SERVICE

The undersigned hereby certifies that on the 21st day of October, 2022, he caused the foregoing DEFENDANT SAMSUNG ELECTRONICS AMERICA, INC.'S MOTION TO DISMISS THE AMENDED CLASS ACTION COMPLAINT to be filed with the Clerk of the District Court via the CM/ECF system, which will send notification of such filing to all counsel of record at the email addresses on file with the Court.

By: /s/ Randall W. Edwards
Randall W. Edwards

ATTORNEY FOR DEFENDANT
SAMSUNG ELECTRONICS AMERICA, INC.

O'MELVENY & MYERS LLP
Randall W. Edwards
Two Embarcadero Center, 28th Floor
San Francisco, CA 94111-3823
(415) 984-8700